



Santa Clara Law Santa Clara Law Digital Commons

Faculty Publications

Faculty Scholarship

1-18-2004

Warez Trading and Criminal Copyright Infringement

Eric Goldman

Santa Clara University School of Law, egoldman@gmail.com

Follow this and additional works at: <http://digitalcommons.law.scu.edu/facpubs>

Automated Citation

Eric Goldman, *Warez Trading and Criminal Copyright Infringement* (2004),
Available at: <http://digitalcommons.law.scu.edu/facpubs/185>

This Article is brought to you for free and open access by the Faculty Scholarship at Santa Clara Law Digital Commons. It has been accepted for inclusion in Faculty Publications by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.

Warez Trading and Criminal Copyright Infringement

By Eric Goldman^{*}

ABSTRACT

Warez traders have been blamed as a significant cause of copyright piracy, which has led to several dozen conviction of warez traders in the past two years. The article analyzes how criminal copyright infringement and other laws apply to warez trading. The article also describes the prosecutions of warez trading, including a comprehensive chart of all warez trading convictions. The article concludes with a brief policy discussion about the problems created by Congress' effort to criminalize warez trading.

TABLE OF CONTENTS

1.	Introduction	page 2
2.	What is Warez Trading?	3
3.	The Criminal Copyright Infringement Statute	5
4.	Elements of a Prosecution and Applicable Defenses	6
	a. Element #1: Valid Copyright	6
	b. Element #2: Infringement	6
	c. Element #3: Willfulness	12
	d. Element #4(a): Commercial Advantage or Private Financial Gain	14
	e. Element #4(b): Retail Value of Infringed Works	15
	f. Statute of Limitations	17
5.	Other Criminal Liability of Warez Trading	17
	a. Anti-Circumvention Laws	17
	b. Anti-Hacking Laws	18
	c. Anti-Theft Laws	19
	d. Trade Secret Protection Laws	20
	e. Copyright Management Information Integrity Laws	20
6.	Criminal Copyright Prosecutions of Warez Traders	21
	a. Jeffrey Levy	22
	b. Eric Thornton	23
	c. Brian Baltutat	23
	d. Fastlane	24
	e. Pirates With Attitude	25
	f. Operations Buccaneer, Bandwidth and Digital Piratez	27
	g. William Fitzgerald	31
	h. Operation Safehaven	31
	i. Operation Cybernet	32
	j. Movie Traders	32

^{*} Eric Goldman (eric.goldman@marquette.edu) is an Assistant Professor at Marquette University Law School in Milwaukee, WI. His personal website is located at http://eric_goldman.tripod.com. The author thanks the participants at DEF CON 11, 2003 Black Hat Briefings and the American Bar Association's 2003 Business Law Section Spring Meeting for their helpful comments, and Ted Potter for his research help.

7. Casualties in the War Against Warez	33
Appendix A: Publicized Convictions Under the No Electronic Theft Act	37

ARTICLE

1. INTRODUCTION.

Warez trading, the non-commercial hobby of collecting and trading copyrighted works (especially software), has been singled out as a major cause of online piracy. In the late 1990s, an industry group claimed that warez trading caused one-third of the world's software piracy losses.¹ More recently, the head of the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) said, "warez groups pose a growing and significant threat to intellectual property rights holders around the world. It is generally agreed that most of the pirated movies, music, games and software available on the Internet come from these high-level warez groups."²

However, legal efforts to control warez trading have been going on for a decade. In 1994, David LaMacchia, a student who operated a bulletin board service for the exchange of copyrighted software, was the first person criminally prosecuted for warez trading. At the time, criminal copyright infringement required infringement for commercial advantage or private financial gain. Because LaMacchia did not have a commercial motive, the government prosecuted him for conspiracy to commit wire fraud instead of criminal copyright infringement.

¹ See Adam L. Penenberg, *Where Do You Want to Pirate Today?*, FORBES, Aug. 8, 1997, available at <http://www.forbes.com/1997/08/08/column.html>.

² *International Copyright Piracy: A Growing Problem with Links to Organized Crime and Terrorism: Hearings Before the Subcomm. on Courts, the Internet and Intellectual Property, House Comm. on the Judiciary*, page 19 (March 13, 2003) (statement of John G. Malcolm, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice), available at http://commdocs.house.gov/committees/judiciary/hju85643.000/hju85643_0.htm;

However, a U.S. Supreme Court case had already declared that copyrighted works were not capable of being taken by fraud,³ so the judge quickly dismissed the case.⁴

After three years of trying, copyright owners finally addressed the perceived hole exposed by LaMacchia's prosecution when Congress enacted the No Electronic Theft (NET) Act (the "NET Act")⁵ in 1997. The NET Act modified criminal copyright law to address LaMacchia's conduct in two principal ways: first, it expanded the definition of "financial gain" to cover bartering implicit in warez trading, and second, it created a new basis of criminal infringement based only on a minimum quantum of infringement (irrespective of motive).

Unquestionably, the NET Act has successfully criminalized most warez trading, and the Department of Justice is adding to its list of successful warez prosecutions at a seemingly ever-increasing rate. Since its passage, over 80 warez traders have been convicted under the NET Act (or analogous doctrines like conspiracy where the underlying claim is a NET Act violation), and 20 of those defendants have received jail sentences. This Article discusses how criminal copyright law applies to warez trading, some enforcement actions under the NET Act, and some policy concerns about criminalizing warez trading.

2. WHAT IS WAREZ TRADING?

The generic term "warez trader" imprecisely lumps together at least four disparate sub-communities within the warez scene. To understand the warez scene, each sub-community must be separately analyzed.

³ Dowling v. United States, 473 U.S. 207 (1985), *available at* <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=473&invol=207>.

⁴ United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994), *available at* http://www.loundy.com/CASES/US_v_LaMacchia.html.

⁵ No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), *available at* <http://www.usdoj.gov/criminal/cybercrime/17-18red.htm>.

Warez distributors are fairly large and organized operations optimized to generate high volumes of new warez quickly.⁶ These operations divide up several discrete tasks among their members, including sourcing new warez, cracking any technological protection devices, testing the cracked warez to make sure they still work, packaging the warez for easy distribution, couriering the warez to propagate the warez to other sites or throughout the Internet, performing systems administration on the computers used by the group, and managing/overseeing the operations.

Warez collectors actively collect and trade warez outside of the distribution groups. They may be trying to gain admission to a warez distribution group or enthusiasts who like showing off trophies.⁷

Warez downloaders do not trade warez per se. Instead, they download warez to use them on a trial or permanent basis. Many warez downloaders just want free software or the latest cutting edge stuff.⁸ However, commercial piracy operations also download warez as new product to press on CDs and sell.⁹

Finally, *abandonware enthusiasts* collect, trade and distribute out-of-print software, particularly games.¹⁰ Some abandonware enthusiasts consider themselves historians or archivists, but in all other respects their actions are indistinguishable from other warez traders.¹¹

⁶ See U.S. Department of Justice, Operation Buccaneer: Illegal “Warez” Organizations and Internet Piracy (July 19, 2002), available at <http://www.cybercrime.gov/ob/OBorg&pr.htm> [hereinafter DOJ Warez Organizations].

⁷ See David McCandless, *Warez Wars*, WIRED, Apr. 1997, available at http://hotwired.wired.com/collections/hacking_warez/5.04_warez_wars_pr.html.

⁸ See Stephen Poole, PC Pirates, CNET GameSpot.com, at 5, at <http://www.gamespot.com/features/pirates/page10.html> (last visited Mar. 7, 2003).

⁹ See, e.g., DOJ Warez Organizations, *supra* note 6.

¹⁰ See Greg Costikyan, *New Front in the Copyright Wars: Out-of-Print Computer Games*, N.Y. TIMES, May 18, 2000, available at <http://www.nytimes.com/library/tech/00/05/circuits/articles/18aban.html>.

¹¹ See David Noack, ‘Abandoned’ Software Issue Draws a Crowd of Opinions, INVESTORS BUS. DAILY, Dec. 8, 2003.

3. THE CRIMINAL COPYRIGHT INFRINGEMENT STATUTE.

Criminal copyright infringement is the willful infringement of a copyright (a) for purposes of commercial advantage or private financial gain (“Section 506(a)(1)”)¹² or (b) by the reproduction or distribution (including by electronic means), during any 180-day period, of copyrighted works with a total retail value of more than \$1,000 (“Section 506(a)(2)”)¹³.

For a first-time violation where the infringement involves reproducing or distributing at least 10 copies with a total retail value of more than \$2,500, criminal penalties include up to 5 years imprisonment (in the case of Section 506(a)(1)) or up to 3 years imprisonment (in the case of Section 506(a)(2)), and in each possibly a fine.¹⁴ Because it offers greater penalties, generally the government prefers to prosecute under Section 506(a)(1).¹⁵ Otherwise, all other criminal infringements can result in up to one year imprisonment and possibly a fine. In all cases, defendants should forfeit the equipment used to commit infringement.¹⁶

The Sentencing Guidelines control the determination of actual sentences, and Section 2B5.3 specifically applies to criminal copyright infringement.¹⁷ In the portions most relevant to warez trading, the guidelines increase the offense level if the infringement involved uploading infringing items (including setting a minimum offense level),¹⁸ decrypting or circumventing technological protection measures to gain access to the work,¹⁹ and participating in an organized

¹² 17 U.S.C. § 506(a)(1), available at <http://www4.law.cornell.edu/uscode/17/506.html>.

¹³ 17 U.S.C. § 506(a)(2), available at <http://www4.law.cornell.edu/uscode/17/506.html>.

¹⁴ 18 U.S.C. § 2319(b) and (c), available at <http://www4.law.cornell.edu/uscode/18/2319.html>. 18 U.S.C. § 3571 (<http://www4.law.cornell.edu/uscode/18/3571.html>) governs the amount of fines.

¹⁵ U.S. Department of Justice, Computer Crime and Intellectual Property Section, Prosecuting Intellectual Property Crimes Manual § III(B)(5) (also noting that a commercial motivation has better jury appeal), available at <http://www.cybercrime.gov/ipmanual/03ipma.htm> [hereinafter DOJ IP Crimes Manual].

¹⁶ 17 U.S.C. § 506(b), available at <http://www4.law.cornell.edu/uscode/17/506.html>.

¹⁷ U.S. SENTENCING GUIDELINES MANUAL § 2B5.3, available at <http://www.ussc.gov/2002guid/2002guid.pdf>.

¹⁸ *Id.* § 2B5.3(b)(2).

¹⁹ *Id.* § 2B5.3 app. 4 (pointing out that § 3B1.3, applicable to the use of special skills, applies).

criminal enterprise.²⁰ Another guideline reduces the offense level when the offense is not committed for commercial advantage or private financial gain.²¹

4. ELEMENTS OF A PROSECUTION AND APPLICABLE DEFENSES.

To convict a defendant of criminal copyright infringement, the government must prove, beyond a reasonable doubt, the following elements: (1) a valid copyright exists, (2) it was infringed, (3) the infringement was willful, and (4) either (a) the infringement was for commercial advantage or private financial gain, or (b) the infringed works' retail value exceeded the statutory thresholds.²²

a. Element #1: Valid Copyright

The government must demonstrate the existence of a valid copyright. Although copyright protection technically attaches when a work is created, the work's copyright must be registered before the work can support a prosecution.²³ If made within five years of the work's publication, registration is *prima facie* evidence that the copyright is valid.²⁴ Even without such a presumption, most warez are derived from works that should have no problem qualifying for copyright protection. As a result, this factor rarely will be relevant in a warez trading case.

b. Element #2: Infringement

A copyrighted work can be infringed, among other ways, through unauthorized reproduction or distribution. Uploading warez to Usenet, IRC, a website or other place where it can be downloaded should constitute both reproduction (making a copy from a local computer to

²⁰ *Id.* § 2B5.3 app. 5(B).

²¹ *Id.* § 2B5.3(b)(3).

²² See generally DOJ IP Crimes Manual, *supra* note 15; A. HUGH SCOTT, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW 263-89 (2001).

²³ 17 U.S.C. § 411(a), available at <http://www4.law.cornell.edu/uscode/17/411.html>.

²⁴ 17 U.S.C. § 410(c), available at <http://www4.law.cornell.edu/uscode/17/410.html>.

the file server) and distribution (when received by downloaders).²⁵ Downloading a file²⁶ and executing the file on a local computer²⁷ should each constitute a reproduction of the file.

While the government can often easily demonstrate that a particular warez item was reproduced or distributed, the government often has some difficulty connecting those activities to a particular defendant. There are several ways the government can try to make that connection, but no method is foolproof:²⁸

- The government can show infringing activity associated with the defendant's username and password, but the defendant can claim that the username and password were stolen or shared.
- The government can show infringing activity associated with an IP address, but the government then must further show that the defendant was using this IP address at the applicable time.
- The government can obtain witness testimony that the defendant committed the infringing acts, but there are rarely "eyewitnessed" accounts of warez trading. However, even if they did not specifically see the defendant engaged in infringement, other group members or undercover agents often can offer damaging testimony.²⁹

²⁵ A&M Records v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) (discussing liability of P2P file traders), *available at* http://www.law.cornell.edu/copyright/cases/239_F3d_1004.htm.

²⁶ *Id.* (discussing liability of P2P file downloaders); In re. Aimster Copyright Litig., 334 F.3d 643, 645 (7th Cir. 2003) (same), *available at* http://www.nmpa.org/pr/Aimster_Opinion_6-30-2003.pdf; Metro-Goldwyn Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1034-35 (C.D. Cal. 2003) (same), *available at* <http://www.law.cornell.edu/copyright/cases/grokster.htm>.

²⁷ It is well accepted that loading a copy into RAM is a reproduction. *See* MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511 (1993), *cert. dismissed*, 510 U.S. 1033 (1994), *available at* http://www.law.cornell.edu/copyright/cases/991_F2d_511.htm.

²⁸ *See generally* DOJ IP Crimes Manual, *supra* note 15, § III(E)(2).

²⁹ *See* Former DrinkOrDie Member Chris Tresco Answers, Slashdot.com, Oct. 4, 2002, *at* <http://interviews.slashdot.org/interviews/02/10/04/144217.shtml?tid=123> (discussing how encrypting email does not help when other group members give their passphrases to the government, making those emails readable).

- The government can obtain evidence from the defendant's computers, although defendants who encrypt or purge data can make this process more difficult.
- Finally, the government can try to prove infringement circumstantially. However, the government generally tries to avoid warez trading prosecutions based solely on circumstantial evidence.

Government-operated or -infiltrated file servers or websites give the government the best opportunity to obtain credible proof connecting a warez trader with infringing activity. This method is obviously difficult for the government, but it has been used successfully in, among others, the Fastlane and Operation Bandwidth (Rogue Warriorz) investigations.³⁰

Warez distributors and collectors can try to minimize liability for distribution by requiring the government to show that an uploaded file was actually downloaded.³¹ However, an infringing distribution can occur merely by making a copy *available* for distribution.³² Further, this defense does not negate liability for copying the file during the upload process.

The First Sale doctrine, which allows redistribution of a legitimately-acquired physical copy of a copyrighted work,³³ is a frequently-raised defense in physical-space criminal copyright cases. However, it offers little help to warez traders because the doctrine only applies to physical copies (not electronic ones)³⁴ and only negates distribution (not reproduction) liability.³⁵

³⁰ See *infra* notes 109 and 142.

³¹ Although the case mostly focused on whether programs were functional, this argument was at issue in determining the proper retail value of the infringed items in the Pirates With Attitude case. See *United States v. Rothberg*, 2002 U.S. Dist. LEXIS 1569 (N.D. Ill. 2002).

³² See *Hotaling v. Church of Jesus Christ of Latter-Day Saints*, 118 F.3d 199, 203 (4th Cir. 1997), available at <http://www.law.emory.edu/4circuit/june97/961399.p.html>. Congressional bills introduced in Summer 2003 are targeted at closing any potential loophole regarding files made available for distribution. See *infra* note 173.

³³ 17 U.S.C. § 109(a), available at <http://www4.law.cornell.edu/uscode/17/109.html>.

³⁴ "Copies" and "phonorecords" both are defined to cover "material objects." 17 U.S.C. § 101, available at <http://www4.law.cornell.edu/uscode/17/101.html>.

³⁵ 17 U.S.C. § 109(a), available at <http://www4.law.cornell.edu/uscode/17/109.html>.

Finally, warez traders will often claim fair use. Fair use is a multi-factor test designed to balance the relatively absolute nature of a copyright monopoly with the social benefits accruing from limited uses of those copyrighted works. The factors are:

- the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- the nature of the copyrighted work;
- the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- the effect of the use upon the potential market for or value of the copyrighted work.³⁶

Because fair use is an equitable defense, courts routinely craft their analyses to support the result they think is appropriate. As a consequence, a fair use defense is highly unpredictable.

Nevertheless, we can make some educated guesses about how courts might apply the factors to warez trading. For example, the second and third factors will usually weigh against a warez trader. The types of files made into warez (software, music, movies) are generally close to copyright's core, and warez traders usually make a complete (or near-complete) copy of each traded work.

The first factor can be a little harder to apply. By definition, warez traders do not infringe for profit. Some commentators have suggested that noncommercial infringement presumptively should be considered fair use,³⁷ which would make noncommercial warez trading immune from prosecution.

³⁶ 17 U.S.C. § 107, available at <http://www4.law.cornell.edu/uscode/17/107.html>.

³⁷ See Lydia P. Loren, *Digitization, Commodification, Criminalization: the Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement*, 77 WASH. U. L. Q. 835, 887 (1999), available at <http://www.wulaw.wustl.edu/WULQ/77-3/773-835.pdf>; James E. Neuman, *Copyright Violations Face Criminal Exposure*, N.Y.L.J., Oct. 13, 2001, at S3; see also DOJ IP Crimes Manual, *supra* note 15, § III(C)(3). In 1984, the Supreme Court said that noncommercial use was presumptively fair, *Sony Corp. v. Universal City Studios*, 464 U.S.

However, the NET Act redefined “financial gain” to include the receipt or expectation of receipt of copyrighted works. Under this definition, many warez traders technically infringe for “financial gain.”³⁸ Thus, in *United States v. Slater*, a warez trader argued that warez trading was noncommercial because traders did not pay to download,³⁹ but the Seventh Circuit soundly rejected this argument, commenting that it “barely pass[es] the straight-face test.”⁴⁰ The *Slater* court said warez trading was a form of barter: the trader contributes valuable services to the warez group in exchange for access to commercially-available software.⁴¹

Alternatively, the Ninth Circuit in *Napster* said that P2P file-sharers infringed for commercial purposes because “repeated and exploitative” copying for personal benefit meant the users could avoid purchasing legitimate copies.⁴² If P2P file traders make “repeated and exploitative” copies, warez traders do too.

In some cases, the court will bypass the commercial-educational spectrum and instead weigh the first factor in favor of fair use when the copy is “transformative,” meaning that it “adds something new, with a further purpose or different character, altering the first with new expression, meaning or message.”⁴³ Although a warez copy may not be identical (due to the removal of copy protection devices, the addition of .nfo files, etc.), these changes do not

417, 449 (1984), available at http://www.law.cornell.edu/copyright/cases/464_US_417.htm, but effectively abandoned this presumption a decade later. See *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 584 (1994), available at <http://supct.law.cornell.edu/supct/html/92-1292.ZS.html>.

³⁸ The *Napster* ruling specifically noted the NET Act’s revised financial gain definition to conclude that P2P file traders engage in commercial infringement under the fair use analysis. *A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1015 (9th Cir. 2001), available at http://www.law.cornell.edu/copyright/cases/239_F3d_1004.htm. Even before the NET Act’s passage, the Department of Justice believed that warez traders’ bartering constituted illegal “financial gain.” See United States Consolidated Response to Defendants’ Pre-Trial Motions, *United States v. Rothberg*, No. 00-CR-85, at 7 n.1 and 11 (N.D. Ill. 2002).

³⁹ *United States v. Slater*, 348 F.3d 666 (7th Cir. 2003), available at <http://www.ca7.uscourts.gov/op3.fwx?submit1=showop&caseno=02-2059.PDF>.

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1015 (9th Cir. 2001), available at http://www.law.cornell.edu/copyright/cases/239_F3d_1004.htm.

⁴³ *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579 (1994), available at <http://supct.law.cornell.edu/supct/html/92-1292.ZS.html>.

“transform” the work into something different. However, some courts have found transformative uses based solely on the resulting work having a different purpose, even if nothing new is added.⁴⁴ Under this approach, warez could have different purposes when they are used for evaluation purposes or as trophies. Nevertheless, unless a court uses a liberal transformative interpretation, warez traders are unlikely to have the first fair use factor weigh in their favor.

The fourth factor is generally regarded as the most important fair use factor,⁴⁵ so a warez trader can go a long way towards establishing a fair use defense if the trader can convince the fact-finder that warez trading does not detrimentally affect the copyright owner’s market. This argument is not completely far-fetched; many warez distributors and collectors never use the warez they trade or archive, and certainly they would never purchase those works.⁴⁶ Thus, a collector who just downloads warez could try to argue that those activities do not adversely affect the market.

Justifying uploading/distribution under the fourth factor is harder. A warez trader could argue that most downloads are made by other warez traders, cycling warez through a group of people who would never buy them. However, some downloaders do use warez as a substitute for the original, in which case those copies could constitute lost sales.⁴⁷ Further, some commercial pirates use warez sites as a source of new inventory.⁴⁸ Even though warez traders usually strongly object to commercial piracy, warez distribution can facilitate commercial piracy and

⁴⁴ See *Kelly v. Arriba Soft Corp.*, 280 F.3d 934 (9th Cir. 2002), available at http://images.chillingeffects.org/cases/Kelly_v_Arriba.html.

⁴⁵ *Harper & Row v. Nation Enters.*, 471 U.S. 539 (1985), available at http://www.law.cornell.edu/copyright/cases/471_US_539.htm.

⁴⁶ See David Pogue, *Some Warez over the Rainbow*, MACWORLD, Oct. 1997, at 3, available at <http://www.macworld.com/1997/10/opinion/3919.html>.

⁴⁷ See generally Jon Healey, *Secret Movie Moguls*, L.A. TIMES, Jan. 7, 2004 (discussing how pirated movies posted to top warez sites filter down to P2P file sharers who may use the files as substitutes for the original).

⁴⁸ See DOJ Warez Organizations, *supra* note 6.

thus detrimentally affect the market for traded works. As a result, many courts will not weigh the fourth factor in favor of warez trading defendants.⁴⁹

Given the nature of their commodity, abandonware traders may have a little more luck on the fourth factor. By definition, abandonware cannot hurt a market that the copyright owner has stopped pursuing. However, some courts protect a copyright owner's choice not to exploit a market,⁵⁰ and in those cases, even the abandonware trader will find little relief under fair use.

Putting aside the technical analysis of the fair use factors, there is little reason to believe that warez trading constitutes fair use. Warez trading is not the type of socially-beneficial behavior that fair use was intended to encourage, so courts are not likely to interpret the defense broadly to help out warez traders. As the Seventh Circuit harshly stated in *Slater*, “[i]t is preposterous to think that [warez trading] is authorized by virtue of the fair use doctrine.”⁵¹

c. Element #3: Willfulness

The government has the burden to prove the defendant's conduct was willful. Willfulness is “a word of many meanings whose construction is often dependent on the context in which it appears.”⁵² In the criminal copyright infringement context, the word's meaning remains unresolved.

There are two different standards used to define “willfulness.” The minority view says that willfulness requires the government to prove only that the defendant had the intent to copy.⁵³ Under this position, warez trading is willful by definition. However, this position has been

⁴⁹ See *United States v. Slater*, 348 F.3d 666 (7th Cir. 2003) (“The government also presented expert testimony on the harmful effect of [warez trading] on the potential market for the copyrighted work, though we think this point is fairly obvious.”), available at <http://www.ca7.uscourts.gov/op3.fwx?submit1=showop&caseno=02-2059.PDF>.

⁵⁰ E.g., *Castle Rock Entm't v. Carol Publ'g Group, Inc.*, 150 F.3d 132 (2d Cir. 1998), available at http://www.law.cornell.edu/copyright/cases/150_F3d_132.htm.

⁵¹ *United States v. Slater*, 348 F.3d 666 (7th Cir. 2003), available at <http://www.ca7.uscourts.gov/op3.fwx?submit1=showop&caseno=02-2059.PDF>.

⁵² *Bryan v. United States*, 524 U.S. 184 (1998), available at <http://supct.law.cornell.edu/supct/html/96-8422.ZS.html>.

⁵³ SCOTT, *supra* note 22, at 277.

heavily criticized,⁵⁴ and language added to Section 506(a)(2) by the NET Act (“evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement”) may have ended any credible argument that the minority position applies to criminal copyright infringement.⁵⁵

The majority view says that willfulness requires the government to prove that the defendant specifically intended to infringe such that the infringement was a voluntary, intentional violation of a known legal duty.⁵⁶ This view creates several additional defenses:

- The defendant (incorrectly) believed in good faith that he or she did not infringe because the original and copy are dissimilar or because of the First Sale doctrine.⁵⁷ This defense offers limited hope to warez traders. As discussed earlier, the First Sale doctrine does not apply to electronic copies, and warez are usually duplicates of the originals. Rarely will these questions be debatable enough to allow a court to conclude that the belief was reasonable.
- The defendant (incorrectly) believed in good faith that the use was fair.⁵⁸ Although in some cases the fair use question could be just debatable enough to support a good faith belief, the Seventh Circuit’s *Slater* opinion (characterizing the fair use defense as “preposterous”) emphatically suggests otherwise.
- The defendant did not know the law.⁵⁹ Criminal copyright infringement laws are technical and opaque, so understandably many warez traders do not understand how their

⁵⁴ Scott characterizes the minority view as “doubtful,” *id.*, and Loren says the minority cases “are not nearly as definite as commentators have made them out to be.” Loren, *supra* note 37, at 877.

⁵⁵ Scott says the added language casts doubts on the minority view’s viability. SCOTT, *supra* note 22, at 277. Nimmer says that the added language precludes any prosecutions based on simple proof of conduct violating the Copyright Act. 4 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 15.02[B][2] (2002).

⁵⁶ SCOTT, *supra* note 22, at 277; NIMMER & NIMMER, *supra* note 55, § 15.02[A][2].

⁵⁷ See NIMMER & NIMMER, *supra* note 55, § 15.02[A][2] (characterizing this as the “better” view).

⁵⁸ See *id.*

⁵⁹ See SCOTT, *supra* note 22, at 278; Loren, *supra* note 37, at 869. See generally DOJ IP Crimes Manual, *supra* note 15, § III(B)(3).

behavior violates the law—and, in fact, warez traders are often incredulous when caught.⁶⁰ However, the defense may apply only if the defendant did not know the laws applicable to *civil* infringement. Warez traders generally know that they are infringing.⁶¹ In fact, committing infringement is a key objective—no reputable warez trader wants to distribute or collect files (like public domain material or open source software) that are freely available to everyone. Because most warez traders know they are doing *something* wrong, this defense will likely fail.

While the majority view of willfulness imposes a reasonably high standard on the government, warez trading is probably willful under either the majority or minority views.

d. Element #4(a): Commercial Advantage or Private Financial Gain

To prosecute under Section 506(a)(1), the government must prove that the infringement was made for commercial advantage or private financial gain. The post-NET Act definition of “financial gain” covers the “receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works.”⁶² Thus, to the extent that a warez trader barter (implicitly or explicitly) copyrighted works, that activity can be characterized as being for financial gain. Although warez traders often trade hundreds or even thousands of copyrighted works, even a single barter suffices.

Some warez traders assert that they share warez without any expectation of return.⁶³ Even so, the Seventh Circuit found financial gain when a warez distribution group member provides services to the group in exchange for access to the warez database.⁶⁴

⁶⁰ See *A Guilty Plea to Violating Copyright Law*, STAR-LEDGER (Newark, N.J.), Dec. 9, 2003 at 33 (quoting the attorney for James Remy).

⁶¹ See David Tetzlaff, *Yo-Ho-Ho and a Server of Warez*, in *THE WORLD WIDE WEB AND CONTEMPORARY CULTURAL THEORY* 115 (Andrew Herman & Thomas Swiss eds. 2000).

⁶² 17 U.S.C. § 101, available at <http://www4.law.cornell.edu/uscode/17/101.html>.

⁶³ See Stephen Granade, Beelzebub Interview, Brasslantern.com, at <http://brasslantern.org/community/interviews/beelzebub.html> (last visited Dec. 1, 2003).

e. Element #4(b): Retail Value of Infringed Works

A felony conviction under Section 506(a)(1) requires the government to prove that the defendant reproduced or distributed copyrighted works with a retail value of at least \$2,500.⁶⁵

Alternatively, prosecutions under Section 506(a)(2) require the government to prove that the defendant, in any 180 period, reproduced or distributed copyrighted works with a retail value over \$2,500 for felony prosecutions⁶⁶ or \$1,000 for misdemeanors.⁶⁷

A copyrighted work can have a number of different “retail” values, ranging from the manufacturer’s list price to the “street” price to the price paid for an infringing copy (which, for warez, is zero). So how is retail value determined? The statute intentionally does not define the term.⁶⁸ While this omission seems problematic, courts will likely refer to the Sentencing Guidelines’ definition of retail value for guidance. That definition sets up a shifting standard for determining retail value: the default is the price paid for the infringing copies,⁶⁹ but the value shifts to the retail value of legitimate copies in (among others) the following circumstances:

⁶⁴ United States v. Slater, 348 F.3d 666 (7th Cir. 2003), available at

<http://www.ca7.uscourts.gov/op3.fwx?submit1=showop&caseno=02-2059.PDF>.

⁶⁵ 18 U.S.C. § 2319(b)(1), available at <http://www4.law.cornell.edu/uscode/18/2319.html>. In addition, the defendant must have reproduced or distributed at least 10 copies of copyrighted works, a standard easily met in most warez cases.

⁶⁶ 18 U.S.C. § 2319(c)(1), available at <http://www4.law.cornell.edu/uscode/18/2319.html>. In addition, the defendant must have reproduced or distributed at least 10 copies of copyrighted works, a standard easily met in most warez cases.

⁶⁷ 18 U.S.C. § 2319(c)(2), available at <http://www4.law.cornell.edu/uscode/18/2319.html>.

⁶⁸ From the House Report accompanying 1992 Copyright Felony Act (the criminal copyright law amendment preceding the NET Act):

The term “retail value” is deliberately undefined, since in most cases it will represent the price at which the work is sold through normal retail channels. At the same time, the Committee recognizes that copyrighted works are frequently infringed before a retail value has been established, and that in some cases, copyrighted works are not marketed through normal retail channels. Examples include motion pictures prints distributed only for theatrical release, and beta-test versions of computer programs. In such cases, the courts may look to the suggested retail price, the wholesale price, the replacement cost of the item, or financial injury caused to the copyright owner.

H.R. REP. 102-997, at 6-7 (1992), available at <http://www.usdoj.gov/criminal/cybercrime/CFAleghist.htm>.

⁶⁹ U.S. SENTENCING GUIDELINES MANUAL § 2B5.3, app. 1, available at <http://www.ussc.gov/2002guid/2002guid.pdf>.

- the infringing item is identical or substantially equivalent to the infringed item, or is a digital or electronic reproduction;
- the infringing item's retail value is difficult or impossible to calculate without unduly complicating or prolonging the proceedings; or
- the infringed item's retail value more accurately assesses the pecuniary harm suffered by the owner.⁷⁰

Based on these factors (especially the first), the retail value used in warez trading cases invariably should be the retail value of legitimate copies.⁷¹ Thus, warez traders should generate high values of infringed works. Indeed, many DrinkOrDie defendants stipulated to infringing works with retail value of between \$2,500,000 and \$5,000,000,⁷² the judge set the retail value for the Pirates With Attitude ("PWA") defendants at \$1,424,640.⁷³ and an individual warez collector recently stipulated to infringing items with a retail value of over \$2.2 million.⁷⁴

In reality, the actual retail value of the copyrighted works infringed by those defendants probably vastly exceeded those amounts. Retail value computations are suppressed by the government's evidentiary challenge of connecting infringing copies with defendants.⁷⁵ Even so,

⁷⁰ *Id.*, § 2B5.3, app. 2.

⁷¹ *See* United States v. Slater, 348 F.3d 666 (7th Cir. 2003) (affirming the district court's decision to equate infringing item's retail value with the infringed item's retail value for Sentencing Guideline purposes because a warez file is the "virtual equivalent" and "digital duplicates" of the infringed software), *available at* <http://www.ca7.uscourts.gov/op3.fwx?submit1=showop&caseno=02-2059.PDF>.

⁷² *See, e.g.*, Press Release, U.S. Department of Justice, Leader of Internet Software Piracy Organization Pleads Guilty to Conspiracy (Feb. 27, 2002), *available at* <http://www.cybercrime.gov/sankusPlea.htm>.

⁷³ United States v. Rothberg, 2002 WL 171963, *6 (N.D. Ill. 2002).

⁷⁴ Press Release, U.S. Department of Justice, Man Admits to Distribution of Pirated Movies, Music, Computer Software and Games Worth Over \$2.2 Million (Dec. 8, 2003), *available at* <http://www.cybercrime.gov/remyPlea.htm>.

⁷⁵ *Id.* (discussing how the district court reduced the number of infringed works from the FBI's proposed number of 34,582 down to 3,947, the number of files on the server when it was seized).

with high dollar values attached to the most attractive warez, most warez traders should easily clear the \$2,500 felony standard.⁷⁶

f. Statute of Limitations

The statute of limitations for criminal copyright infringement is five years.⁷⁷ So far, most cases appear to be brought well before that, as stale cases pose extra evidentiary challenges.

5. OTHER CRIMINAL LIABILITY OF WAREZ TRADING.

Congress has created several new intellectual property crimes in the past decade, giving the government more tools to prosecute warez traders than were available during LaMacchia's prosecution. Therefore, even if the government cannot or does not want to prosecute a warez trader for copyright infringement, the trader may not be off the hook.⁷⁸ Alternatively, the government may bring multiple charges against a defendant to increase the defendant's incentives to plead guilty.⁷⁹

a. Anti-Circumvention Laws

In 1998, Congress passed the Digital Millennium Copyright Act (DMCA) prohibiting the circumvention of technological measures that effectively control access to a copyrighted work⁸⁰ and the making of or trafficking in a device that circumvents such technological measures.⁸¹

⁷⁶ Even smaller players like Levy, Thornton and Fitzgerald easily cleared the felony threshold (stipulating to \$5,000, \$9,638 and over \$40,000, respectively). See *infra* notes 100, 102 and 150.

⁷⁷ 17 U.S.C. § 507(a), available at <http://www4.law.cornell.edu/uscode/17/507.html>.

⁷⁸ Of course, warez traders can be civilly sued for copyright infringement as well.

⁷⁹ See William J. Stuntz, *The Pathological Politics of Criminal Infringement*, 100 MICH. L. REV. 505, 520 (2001) (calling this practice "charge-stacking").

⁸⁰ 17 U.S.C. § 1201(a)(1), available at <http://www4.law.cornell.edu/uscode/17/1201.html>.

⁸¹ 17 U.S.C. § 1201(a)(2) and § 1201(b), available at <http://www4.law.cornell.edu/uscode/17/1201.html>. This law was used to prosecute David Rocci for distributing and selling mod chips that allowed games warez to be played on game consoles. See Press Release, U.S. Department of Justice, Justice Department Seizes Top Internet Site Involved in Copyright Piracy (Feb. 26, 2003), available at <http://www.usdoj.gov/criminal/cybercrime/rocciPlea.htm>.

Punishments for the first offense include imprisonment of up to five years and a fine of up to \$500,000.⁸²

Every major warez distribution group has at least one cracker who specializes in disabling or bypassing copyright protection devices.⁸³ The cracker's behavior should violate the DMCA, and other group members can be prosecuted as conspirators or aiders/abettors. While there are some exceptions to the law,⁸⁴ these exceptions are very technical in nature, and a typical warez trader cannot credibly argue that the exceptions apply.

b. Anti-Hacking Laws

The Computer Fraud and Abuse Act (the "CFAA"),⁸⁵ historically designed as an anti-hacking statute, has become a general-purpose federal anti-trespassing law applicable to warez trading in at least two ways.

First, the CFAA criminalizes accessing computer systems without authorization to obtain information,⁸⁶ a provision that could apply to illegitimately obtaining warez from a copyright owner's computer system. For example, the CFAA may have been violated when a PWA group member allowed other members to take software from Microsoft's internal computer network.⁸⁷ Punishment for the first offense can include imprisonment of up to five years and a fine if the act was committed for commercial advantage or private financial gain, if the taken information's

⁸² 17 U.S.C. § 1204, available at <http://www4.law.cornell.edu/uscode/17/1204.html>.

⁸³ See DOJ Warez Organizations, *supra* note 6.

⁸⁴ 17 U.S.C. § 1201(d)-(j), available at <http://www4.law.cornell.edu/uscode/17/1201.html>. These exceptions cover libraries and universities, law enforcement, reverse engineering (in very limited circumstances), encryption research (in very limited circumstances), devices that protect minors from accessing harmful material on the Internet, the circumvention of devices to protect personal information, and security testing (in very limited circumstances).

⁸⁵ 18 U.S.C. § 1030, available at <http://www4.law.cornell.edu/uscode/18/1030.html>.

⁸⁶ 18 U.S.C. § 1030(a)(2)(C), available at <http://www4.law.cornell.edu/uscode/18/1030.html>. Portions of the Electronic Communications Privacy Act could also apply if the conduct involves hacking into email servers to obtain emails. 18 U.S.C. § 2701, available at <http://www4.law.cornell.edu/uscode/18/2701.html>.

⁸⁷ See Press Release, U.S. Department of Justice, U.S. Indicts 17 in Alleged International Software Piracy Conspiracy (May 4, 2000), available at <http://www.usdoj.gov/criminal/cybercrime/pirates.htm>.

value exceeded \$5,000, or if the act furthered other crimes or torts (such as copyright infringement).⁸⁸

Second, the CFAA criminalizes accessing computer systems without authorization and causing damage.⁸⁹ In the warez context, this provision could apply to the use of third party computer networks without authorization to distribute warez or conduct group business (with the damage being the use of network resources or the security measures taken to abate the intrusion). Punishment for the first offense can include imprisonment of up to five years and a fine if the damage was caused “recklessly.”⁹⁰

In addition to the federal CFAA, many states have anti-hacking or anti-computer trespass statutes that would allow state prosecutors to bring suit against warez traders for the same behavior.

c. Anti-Theft Laws

A warez trading operation may involve the theft of physical items. For example, Intel employees exchanged stolen Intel servers for access to PWA’s warez database.⁹¹ At a minimum, the Intel employees could be prosecuted for theft, and the other PWA members could be prosecuted for receiving stolen property or participating in a conspiracy to commit theft.

⁸⁸ 18 U.S.C. § 1030(c)(2), available at <http://www4.law.cornell.edu/uscode/18/1030.html>.

⁸⁹ 18 U.S.C. § 1030(a)(5)(A), available at <http://www4.law.cornell.edu/uscode/18/1030.html>. 18 U.S.C. § 1030(a)(4) may also apply if the conduct was done knowingly with the intent to defraud and the value of the network usage exceeds \$5,000 in a year.

⁹⁰ 18 U.S.C. § 1030(c)(4)(B), available at <http://www4.law.cornell.edu/uscode/18/1030.html>. The same penalties applies if the prosecution is brought under 18 U.S.C. § 1030(a)(4).

⁹¹ Press Release, U.S. Department of Justice, U.S. Indicts 17 in Alleged International Software Piracy Conspiracy (May 4, 2000), available at <http://www.usdoj.gov/criminal/cybercrime/pirates.htm>.

d. Trade Secret Protection Laws

In 1996, Congress passed the Economic Espionage Act,⁹² which in practice has established a federal anti-trade secret misappropriation statute. Many states also have their own anti-misappropriation criminal laws. These laws could apply to warez trading of any pre-release software versions (whether alpha, beta or golden master versions) that qualify as trade secrets, which should include many of the most coveted “0-day” warez.

e. Copyright Management Information Integrity Laws

While the DMCA’s anti-circumvention provisions receive most of the media’s attention, another provision of the DMCA—regarding the “integrity of copyright management information”—also could apply to warez trading. Copyright management information (“CMI”) includes, among other things, a copyrighted work’s title, author and other named contributors (“credits”), user agreement and identifying numbers like ISBN or serial numbers.⁹³

The CMI integrity provisions prohibit providing (or distributing or importing for distribution) false CMI “knowingly and with the intent to induce, enable, facilitate, or conceal infringement.”⁹⁴ They also prohibit removing or altering CMI, or distributing (or importing for

⁹² 18 U.S.C. §§ 1831-39, available at <http://www4.law.cornell.edu/uscode/18/pIch90.html>. Section 1832 most specifically applies to warez trading.

⁹³ Copyright Management Information is defined as “(1) the title and other information identifying the work, including the information set forth on a notice of copyright, (2) the name of, and other identifying information about, the author of a work, (3) the name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright, (4) with the exception of public performances of works by radio and television broadcast stations, the name of, and other identifying information about, a performer whose performance is fixed in a work other than an audiovisual work, (5) with the exception of public performances of works by radio and television broadcast stations, in the case of an audiovisual work, the name of, and other identifying information about, a writer, performer, or director who is credited in the audiovisual work, (6) terms and conditions for use of the work, (7) identifying numbers or symbols referring to such information or links to such information, and (8) such other information as the Register of Copyrights may prescribe by regulation, except that the Register of Copyrights may not require the provision of any information concerning the user of a copyrighted work.” 17 U.S.C. § 1202(c), available at <http://www4.law.cornell.edu/uscode/17/1202.html>.

⁹⁴ 17 U.S.C. § 1202(a), available at <http://www4.law.cornell.edu/uscode/17/1202.html>.

distribution) CMI knowing it has been improperly removed or altered.⁹⁵ Punishments mirror those applicable to the anti-circumvention provisions: for the first offense, imprisonment of up to five years and a fine of up to \$500,000.⁹⁶

Warez trading can implicate the CMI integrity provisions in two ways. First, crackers may remove or alter CMI during the crack. Second, adding a .nfo file could be interpreted as providing false CMI with the intent to induce or enable infringement. The .nfo file's wording may make a difference, but claiming "authorship" of a crack could be a violation. Once again, all participants in a group should have joint liability for violation, either directly for distributing the CMI or indirectly as conspirators or aiders/abettors.

6. CRIMINAL COPYRIGHT PROSECUTIONS OF WAREZ TRADERS.

As discussed in Section 4, warez traders have few viable defenses to a criminal copyright prosecution. Not surprisingly, scores of warez traders have been successfully convicted of criminal copyright infringement. Appendix A provides a table of publicized warez-related prosecutions that have resulted in a conviction.

Significantly, the Department of Justice has won every publicized case they have brought under the NET Act, reflecting typical department care in selecting defendants and preparing cases. Not coincidentally, almost all warez trading defendants plead guilty when charged. At least some defendants do so to reduce their sentences.⁹⁷ Others may plead because of the warez trading ethos; traders know that they are playing a game that involves both winning and losing and thus may willingly accept losing if they feel the Feds outsmarted them. Whatever the

⁹⁵ 17 U.S.C. § 1202(b), available at <http://www4.law.cornell.edu/uscode/17/1202.html>. In addition to the DMCA's CMI integrity provisions, the Copyright Act separately prohibits, with fraudulent intent, placing a false copyright notice, 17 U.S.C. § 506(c), available at <http://www4.law.cornell.edu/uscode/17/506.html>, or removing or altering a copyright notice. 17 U.S.C. § 506(d), available at <http://www4.law.cornell.edu/uscode/17/506.html>. Because the associated punishment is only a \$2,500 fine, these provisions are rarely enforced.

⁹⁶ 17 U.S.C. § 1204, available at <http://www4.law.cornell.edu/uscode/17/1204.html>.

⁹⁷ See U.S. SENTENCING GUIDELINES MANUAL § 3E1.1, available at <http://www.ussc.gov/2002guid/2002guid.pdf>.

reasons, only two warez traders, Christian Morley (PWA) and Tony Walker (Fastlane) have taken their case to a jury, and both lost.

As of November 1, 2003, at least 20 of the warez trading defendants listed in Appendix A have received jail sentences. Of those defendants, the (initial) average length is approximately 25.7 months; the longest jail sentence was 46 months and the shortest was 4 months.⁹⁸ It is hard to draw many conclusive inferences about why sentences vary, except that generally a warez group leader gets the harshest sentence and mere participants (as opposed to leaders) often get probation instead of jail time.

Some specific details about the publicized prosecutions:

a. Jeffrey Levy

In August 1999, Jeffrey Levy, a 22 year old University of Oregon senior, became the first individual convicted under the NET Act. He was a small-time trader of music, movies and traditional warez. A “conservative estimate” of his warez’s retail value was \$70,000.⁹⁹ but he pleaded guilty to distributing warez with a retail value of at least \$5,000 and was sentenced to 2 years probation.¹⁰⁰

As a minor warez trader, normally Levy would have escaped prosecutorial attention. However, three months prior to his arrest, Congress angrily demanded that the government deliver some convictions under the NET Act,¹⁰¹ and Levy appears to have been a timely and easy target.

⁹⁸ Note that these calculations are based on the initial sentence. Some defendants, especially DrinkOrDie group members, subsequently received reduced sentences, presumably due to their cooperation with the government.

⁹⁹ Press Release, U.S. Department of Justice, Defendant Sentenced for First Criminal Copyright Conviction Under the “No Electronic Theft” (NET) Act for Unlawful Distribution of Software on the Internet (Nov. 23, 1999), available at <http://www.cybercrime.gov/levy2rls.htm>.

¹⁰⁰ *Id.*

¹⁰¹ At a hearing of the House Judiciary Committee’s Subcommittee on Courts and Intellectual Property in May 1999, Rep. Coble demanded to know why there had been no convictions under the NET Act in 18 months despite the industry lobbyists’ arguments that “there is no shortage of potential prosecutions that could be pursued under the

b. Eric Thornton

Eric John Thornton, another small warez trader who operated a website called “No Patience,” was the second person convicted under the NET Act. In one specific instance, a third party downloaded 20 software programs with a retail value of \$9,638.¹⁰² Thornton pleaded guilty to a misdemeanor violation of the NET Act¹⁰³ and was sentenced to five years probation.¹⁰⁴ In an unusual twist, he had to post a cautionary tale on his website for 18 months.¹⁰⁵ Thornton’s prosecution resembles Levy’s in import and timing, suggesting that both prosecutions were hurriedly initiated in response to Congress’ demands but Thornton’s prosecution just took longer than Levy’s.

c. Brian Baltutat

Brian Baltutat was a slightly more substantial warez trader than Levy or Thornton. He operated a website called “Hacker Hurricane” that offered 142 software programs for

Act.” *Oversight Hearing on the Implementation of the NET Act and Enforcement Against Internet Piracy Before the House Judiciary Committee’s Subcomm. on Courts and Intellectual Property* (May 12, 1999) (statement of Rep. Coble), available at <http://www.house.gov/judiciary/cobl0512.htm>.

¹⁰² Press Release, U.S. Department of Justice, Virginia Man Pleads Guilty to Charges Filed Under the “No Electronic Theft” (NET) Act for Unlawful Distribution of Software on the Internet (Dec. 22, 1999), available at <http://www.cybercrime.gov/thornton.htm>.

¹⁰³ Bill Miller, *Giveaways Costly for Web Pirate*, WASH. POST, Dec. 23, 1999, at B1.

¹⁰⁴ *Internet Pirate to Pay Restitution*, WASH. POST, Mar. 4, 2000, at B2.

¹⁰⁵ Miller, *supra* note 103, at B1. The announcement, perhaps ghost-written by the Department of Justice, reads:

All you WaReZ ToadZ out there need to read this!!!

I am out of the WaReZ business. I have been contributing to the WaReZ scene for some time. OK!

OK! I guess I knew it was illegal - but hell, everyone was doing it.

One day, I was minding my own business at home when I heard a knock on my door. When I opened it, I was staring at gold badges being held by two FBI agents. They explained to me that I had been committing federal copyright infringement. They had been investigating my website with the assistance of the Business Software Alliance. They had even seized evidence from my ISP. Since I was facing a very serious felony charge I came clean with them. I was charged and now have a federal conviction.

I didn’t think anyone cared about WaRez distribution on the Internet.

Boy! Was I wrong!

downloading and was visited by 65,000 people.¹⁰⁶ He was sentenced to 3 years probation and 180 days home confinement.¹⁰⁷

d. Fastlane

In February 2001, the government finally scored a major bust by arresting nine members of the warez distribution group Fastlane.¹⁰⁸ The FBI infiltrated the group by setting up and surreptitiously operating a computer site known as Super Dimensional Fortress Macros (SDFM).¹⁰⁹ SDFM had 697 gigabytes uploaded and 1.9 terabytes downloaded between January to September 2000, with a total retail value over \$1 million.¹¹⁰

All defendants were charged with one count of conspiracy to commit copyright infringement, and eight were charged with one count of committing copyright infringement.¹¹¹ Eight of the nine defendants pleaded guilty, while one defendant (Tony Walker) was found guilty at a jury trial.¹¹² Three defendants received jail sentences ranging from five to thirty months,¹¹³ and the others received probation of three years.

¹⁰⁶ Press Release, U.S. Department of Justice, Man Sentenced in Michigan for Offering Software Programs for Free Downloading on "Hacker Hurricane" Web Site (Jan. 30, 2001), *available at* <http://www.cybercrime.gov/baltutatsent.htm>.

¹⁰⁷ *Id.*

¹⁰⁸ The individual Fastlane defendants are:

Ryan Breeding, aka "river," 26, of Oklahoma City, OK.

Steve Deal, aka "Doobie" and "Dewbie," 36, of Trenton, NJ.

Glendon Martin, aka "TeRRiFiC," 25, of Garland, TX.

Shane McIntyre, aka "Crypto," 22, of Boynton Beach, FL.

James Milne, aka "lordchaos" and "lc," 19, of Shawnee, KN.

Bjorn Schneider, aka "airwalker," "a|walker" and "aw," 20, of Falmouth, MA.

Kevin Vaughan, aka "DaBoo," 19, of Raleigh, NC.

Tony Walker, aka "SyS," 31, of San Diego, CA.

Tae Yuan Wang, aka "Terry Wang" and "Prometh," 19, of Bellevue, WA.

Press Release, U.S. Department of Justice, Nine Indicted in Chicago in \$1 Million "Fastlane" Software Piracy Conspiracy (Feb. 16, 2001), *available at* <http://www.cybercrime.gov/fastlane.htm>.

¹⁰⁹ *Id.*

¹¹⁰ *Id.* Other Fastlane-associated websites include Sacred Halls (SH) (operated by Milne), The Good News (TGN) (operated by Martin) and 4:20 (operated by Vaughan). *Id.*

¹¹¹ *Id.* Kevin Vaughan was not charged with committing copyright infringement.

¹¹² See United States v. Deal, No. 00-CR-774-8 (N.D. Ill. 2002).

¹¹³ See *id.*

e. Pirates With Attitude

After Fastlane, PWA¹¹⁴ was the next major warez distribution group busted. The group operated 13 FTP servers, with its flagship site Sentinel housed at the University of Sherbrooke.¹¹⁵ Sentinel had over 30,000 warez and more than 100 users.¹¹⁶

Seventeen defendants were indicted: twelve PWA members and five Intel employees who supplied computer hardware in exchange for access rights to the warez servers.¹¹⁷ Following the indictments, many defendants entered into plea agreements. The government then claimed the warez had a retail value of over \$10 million.¹¹⁸ A group of defendants jointly moved to limit this retail value based on expectations the defendants formed while negotiating their plea

¹¹⁴ The individual Pirates With Attitude defendants are:

Convicted members of Pirates With Attitude:
Steven Ahnen, aka "Code3," 44, of Sarasota, FL.
Diane Dionne, aka "Akasha," 41, of West Palm Beach, FL.
Christian Morley, aka "Mercy" 29, of Salem, MA.
Thomas Oliver, aka "Rambone," 36, of Aurora, IL.
Jason Phillips, aka "Corv8," 31, of Plano, TX.
Justin Robbins, aka "Warlock," 26, of Lake Station, IN (Microsoft employee).
Robin Rothberg, aka "Marlenus," 34, of Newburyport, MA.
Jason Slater, aka "Technic," 31, of Sunnyvale, CA.
Mark Stone, aka "Stoned," 36, of Fountain Valley, CA.
Todd Veillette, aka "Gizmo," 42, of Oakdale, CT.

Convicted Intel employees:
Tyrone Augustine, 30, of New Rochelle, NY.
Brian Boyanovsky, aka "Boynger," 26, of Aloha, OR.
John Geissberger, 39, of Knoxville, TN.
Brian Riley, 32, of Portland, OR.
Gene Tacy, 27, of Hampstead, NH.

Fugitive members of Pirates With Attitude:
Kaj Bjorlin, aka "Darklord," Sweden.
Mark Veerboken, aka "Shiffie," Belgium.
Press Release, U.S. Department of Justice, Leader Of Software Piracy Sentenced To 18 Months In Prison (May 15, 2002), available at http://www.cybercrime.gov/rothbergSent_pirates.htm [hereinafter Rothberg Sentenced Press Release]. See generally *United States v. Rothberg*, No. 00-CR-85 (N.D. Ill. 2002); Special November 1999 Grand Jury Indictment, *United States v. Rothberg*, No. 00-CR-85 (N.D. Ill. 2002).

¹¹⁵ Rothberg Sentenced Press Release, *supra* note 114.

¹¹⁶ *Id.*

¹¹⁷ *Id.*

¹¹⁸ *United States v. Rothberg*, 2002 WL 171963, *1 (N.D. Ill. 2002).

agreements. The judge rejected the motion but permitted defendants to rescind their plea agreements, and thus withdraw their guilty pleas, if they chose to.¹¹⁹ None did.¹²⁰

A group of defendants then petitioned the court to set a lower retail value. Using a series of questionable estimates, the court set the value at \$1,424,640,¹²¹ a calculation upheld by the Seventh Circuit.¹²² With the retail value established, individual defendants were sentenced.

Robin Rothberg, the PWA leader, entered a blind guilty plea¹²³ but requested downward departure from the Sentencing Guidelines.¹²⁴ After obtaining some relief from the court on that front, he was sentenced to eighteen months in prison.¹²⁵

Another PWA member, Christian Morley, did not negotiate a plea agreement and instead took his case to trial. A jury found him guilty, and he received two years in prison.¹²⁶ On appeal, Morley challenged the judge's failure to provide a jury instruction regarding fair use, but the Seventh Circuit affirmed this omission.¹²⁷

Two other defendants, Jason Slater and Justin Robbins, received jail sentences of eight months and seven months, respectively.¹²⁸ Nine defendants received 5 years probation, and two defendants (Thomas Oliver and Steven Ahnen) each received 3 years probation.¹²⁹ Two defendants remain at large.¹³⁰

¹¹⁹ United States v. Rothberg, 2001 WL 1654758 (N.D. Ill. 2001).

¹²⁰ United States v. Rothberg, 2002 WL 171963, *2 (N.D. Ill. 2002).

¹²¹ *Id.* at *6.

¹²² United States v. Slater, 348 F.3d 666 (7th Cir. 2003), available at <http://www.ca7.uscourts.gov/op3.fwx?submit1=showop&caseno=02-2059.PDF>

¹²³ A "blind" plea is made without the benefit of a plea agreement. United States v. Rothberg, 222 F. Supp. 2d 1009, 1012 (N.D. Ill. 2002).

¹²⁴ *Id.* Rothberg received a 2 level downward revision based on his absence of a profit motive, his extraordinary acceptance of responsibility and his family circumstances. *Id.*

¹²⁵ Rothberg Sentenced Press Release, *supra* note 114.

¹²⁶ *Id.*

¹²⁷ United States v. Slater, 348 F.3d 666 (7th Cir. 2003), available at <http://www.ca7.uscourts.gov/op3.fwx?submit1=showop&caseno=02-2059.PDF>.

¹²⁸ See United States v. Rothberg, No. 00-CR-85 (N.D. Ill. 2002).

¹²⁹ See *id.*

¹³⁰ The fugitives are Mark Veerboken and Kaj Bjorlin. Rothberg Sentenced Press Release, *supra* note 114.

f. Operations Buccaneer, Bandwidth and Digital Piratez

Operations Buccaneer, Bandwidth and Digital Piratez were major government operations targeting warez distribution groups that, on December 11, 2001, led to the execution of approximately 100 search warrants in the U.S., Canada, the United Kingdom, Australia, Sweden, Norway and Finland.¹³¹

¹³¹ Press Release, U.S. Department of Justice, Federal Law Enforcement Targets International Internet Piracy Syndicates (Dec. 11, 2001), available at <http://www.cybercrime.gov/warezoperations.htm>.

Operation Buccaneer¹³² primarily targeted DrinkOrDie, one of the oldest and best-known warez distribution groups.¹³³ Among other accomplishments, the group claimed to have released

¹³² Individual defendants prosecuted pursuant to Operation Buccaneer include:

Richard Berry, aka "Flood," 34, of Rockville, MD (VP and CTO at Streampipe.com).
 Anthony Buchanan, aka "spaceace," of Eugene, OR.
 Andrew Clardy, 49, aka "DooDad," of Galesburg, IL (network technician at Carl Sandburg College).
 Myron Cole, aka "t3rminal," of Warminster, PA.
 Derek Eiser, aka "Psychod," of Philadelphia, PA.
 Barry Erickson, aka "rads1," 35, of Eugene, OR (systems engineer at Symantec Corporation).
 Hew Raymond Griffiths, aka "Bandido," 40, of Bateau Bay, Australia.
 David A Grimes, aka "Chevelle," 25, of Arlington, TX (computer engineer at Check Point Software).
 Robert Gross, aka "targetpractice," of Horsham, PA.
 Nathan Hunt, aka "Azide," 25, of Waterford, PA.
 Kentaga Kartadinata, aka "Tenkuken," 29, of Los Angeles, CA.
 Michael Kelly, aka "Erupt," 21, of Miami, FL (network administrator for Gator Leasing).
 Stacey Nawara, aka "Avec," 34, of Rosenberg, TX.
 Mike Nguyen, aka "Hackrat," 26, of Los Angeles, CA.
 Sabuj Pattanayek, aka "Buj," 20, of Durham, NC.
 Shane Pitman, aka "Pitbull," 31, of Conover, NC.
 John Riffe, aka "blue" or "blueadept," 32, of Port St. John, FL.
 David Russo, aka "Ange," 49, of Warwick, RI.
 John Sankus, aka "eriFleH," 28, of Philadelphia, PA.
 Mark Shumaker, aka "markalso," 21, of Orlando, FL.
 Kirk Patrick St. John, aka "thesaint," 34, of Gilbert, AZ.
 Christopher Tresco, aka "BigRar," 23, of Boston, MA (MIT systems administrator).
 Press Release, U.S. Department of Justice, Warez Leader Sentenced to 46 Months (May 17, 2002), *available at* <http://www.cybercrime.gov/sankusSent.htm>; U.S. Department of Justice, Operation Buccaneer Defendants (Jan. 27, 2003), *available at* <http://www.cybercrime.gov/ob/Dchart.htm>; Press Release, U.S. Department of Justice, Defendant Indicted in Connection with Operating Illegal Internet Software Piracy Group (Mar. 12, 2003), *available at* <http://www.cybercrime.gov/griffithsIndict.htm>; Press Release, U.S. Department of Justice, Warwick Man Admits Participation in Software Piracy Network (Apr. 24, 2003), *available at* <http://www.cybercrime.gov/russoPlea.htm>; Press Release, U.S. Department of Justice, Former Leader of Razor 1911, the Oldest Game Software Piracy Ring on the Internet, Sentenced (June 6, 2003), *available at* <http://www.cybercrime.gov/pitmanSent.htm>; Press Release, U.S. Department of Justice, Valley Man Indicted in International Software Piracy Scheme (Nov. 26, 2003), *available at* <http://www.cybercrime.gov/stjohnIndict.htm>.

Specific sentences are described in *United States v. Berry*, No. 02-CR-246 (E.D. Va. 2003); *United States v. Buchanan*, No. 02-CR-374 (E.D. Va. 2003); *United States v. Clardy*, No. 02-CR-10035 (C.D. Ill. 2003); *United States v. Cole*, No. 02-CR-300 (E.D. Va. 2003); *United States v. Eiser*, No. 02-CR-284 (E.D. Va. 2003); *United States v. Erickson*, No. 02-CR-89 (E.D. Va. 2003); *United States v. Gross*, No. 02-CR-299 (E.D. Va. 2003); *United States v. Hunt*, No. 02-CR-106 (E.D. Va. 2003); *United States v. Kelly*, No. 02-CR-112 (E.D. Va. 2003); *United States v. Nawara*, No. 02-CR-90 (E.D. Va. 2003); *United States v. Nguyen*, No. 02-CR-63 (C.D. Cal. 2003); *United States v. Pattanayek*, No. 02-CR-118 (E.D. Va. 2003); *United States v. Riffe*, No. 02-CR-156 (E.D. Va. 2003); *United States v. Tresco*, No. 02-CR-132 (E.D. Va. 2003).

¹³³ Fact Sheet, U.S. Customs Service, The DrinkOrDie Group: What is It? Who Are They? What is the DrinkOrDie Group? (Dec. 11, 2001), *available at* <http://www.customs.ustreas.gov/hot-new/pressrel/2001/1211-01.htm>. *But see* Farhad Manjoo, Were DrinkOrDie Raids Overkill?, *Wired News* (Dec. 13, 2001), *at* <http://www.wired.com/news/print/0,1294,49096,00.html> (arguing that "DrinkOrDie was small potatoes in the world of software theft"). Other groups targeted by Operation Buccaneer include Razor1911, RiSCISO, MYTH, POPZ, RequestToSend (RTS), WeLoveWarez (WLW), and RiSC. U.S. Department of Justice, Operation Buccaneer: The Investigation (July 19, 2002), *available at* <http://www.cybercrime.gov/ob/OBinvest.htm>.

Microsoft Windows 95 two weeks prior to its commercial release.¹³⁴ The group allegedly had two leaders, two or three council members, twelve to fifteen staff members, and approximately 65 general members.¹³⁵ The groups' archives contained, in some cases, two terabytes of warez estimated to have a retail value of hundreds of millions of dollars.¹³⁶ However, as part of plea agreements, many Operation Buccaneer defendants admitted that the retail value was between \$2.5 million and \$5 million.¹³⁷

In conjunction with Operation Buccaneer, Mark Shumaker pleaded guilty to operating the Apocalypse Crew site, which contained pre-release digital music files solicited from DJs and reviewers.¹³⁸ Shumaker also admitted to uploading and downloading infringing files from DrinkOrDie servers, and his total infringement was stipulated at \$40,000-\$70,000.¹³⁹

Of the 19 Operation Buccaneer defendants on Appendix A sentenced as of November 1, 2003, eleven received jail sentences ranging from 18 to 46 months (although at least ten of these defendants had their sentences reduced in exchange for government cooperation), three received five years probation, one received one year probation and the other four received two years probation.

¹³⁴ Fact Sheet, U.S. Customs Service, The DrinkOrDie Group: What is It? Who Are They? What is the DrinkOrDie Group? (Dec. 11, 2001), available at <http://www.customs.ustreas.gov/hot-new/pressrel/2001/1211-01.htm>.

¹³⁵ Statement of Facts, United States v. Tresco, No. 02-CR-132-A, at 2 (E.D. Va. 2002).

¹³⁶ U.S. Department of Justice, Operation Buccaneer: The Investigation (July 19, 2002), available at <http://www.cybercrime.gov/ob/OBinvest.htm>. A single file server operated by DrinkOrDie, Fatal Error, was alleged to have over 900 gigabytes and 15,000 titles of software. Criminal Information, United States v. Tresco, No. 02-CR-132-A, at 3 (E.D. Va. 2002).

¹³⁷ See, e.g., Plea Agreement, United States v. Tresco, No. 02-CR-132-A, at 2 (E.D. Va. 2002); Software Pirate Pleads Guilty, GlobeandMail.com, Apr. 4, 2002, at http://www.globeandmail.com/servlet/RTGAMArticleHTMLTemplate?tf=RT/fullstory_print.html&cf=RT/config-neutral&slug=gtcopy&date=20020404&archive=RTGAM&site=Technology; Press Release, U.S. Department of Justice, Leader of Internet Software Piracy Organization Pleads Guilty to Conspiracy (Feb. 27, 2002), available at <http://www.cybercrime.gov/sankusPlea.htm>.

¹³⁸ See Press Release, U.S. Department of Justice, Online Music Piracy Leader Pleads Guilty (Aug. 21, 2003), available at <http://www.usdoj.gov/criminal/cybercrime/shumakerPlea.htm>; see also Statement of Facts, United States v. Shumaker, Crim. No. 03-326-A (E.D. Va. 2003), available at <http://www.usdoj.gov/usao/vae/ArchivePress/AugustPDFArchive/shumakersof082103.pdf>.

¹³⁹ Statement of Facts, United States v. Shumaker, Crim. No. 03-326-A (E.D. Va. 2003), available at <http://www.usdoj.gov/usao/vae/ArchivePress/AugustPDFArchive/shumakersof082103.pdf>.

Operation Bandwidth¹⁴⁰ primarily targeted Rogue Warriorz (RWZ), another major warez distribution group. The group required membership applications and recorded statistics for group members who had maintained and moved the greatest number of files.¹⁴¹ Undercover FBI, EPA and Defense Criminal Investigative Services agents infiltrated the group's Shatnet site,¹⁴² which contained over 9,000 warez with a retail value of approximately \$7 million.¹⁴³ As of January 1, 2004, at least 19 Operation Bandwidth defendants have pleaded guilty and at least 5 of those have been sentenced, all to probation.

¹⁴⁰ Individual defendants prosecuted pursuant to Operation Bandwidth include:

John J. Amorosi, aka "Sloanman", 22, of Falls Church, VA.
 Wolf Bachenor, aka Walter Bachenor, aka "Drinfotheif", "DrinfoTHV" and "Doctor", 51, of Park Slope, NY.
 David Brandt, aka "Bocephus", 35, of Wake Village, TX.
 Alexander Castaneda, aka "Prentice" and "Alex", 20, of Federal Way, WA.
 Jacob Paul Clapton, aka "Axxess", 29, of Livermore, CA.
 Lukasz Doupal, aka "Luk@s", 24, of Brooklyn, NY.
 Jonathan Dow, aka "Demon Furby", 34, of Iliion, NY.
 Jorge Garcia, Jr., aka "Lh" and "Lordhacker", 29, of Reddick, FL.
 Bryan Ray Harshman, aka "Carrier", 22, of St. Joseph, MO.
 Mark Konarske, aka "Markus" and "Markruss", 41, of Flat Rock, MN.
 Timothy J. Lastoria, aka "Waldorf", 24, of Brecksville, OH.
 Ruth Lawton
 David Lowe, aka "Dragon", 41, of Akron, OH.
 Christopher Mastrangelo, aka "Floyd", 31, of Toms River, NJ.
 Brad McGourty
 Michael Meacham, aka "Dvorak", 35, of Barberton, OH
 Suzanne Peace, aka "Peaces", 37, of Lombard, IL.
 Lindle Romero, aka "Rahman", 37, of Houston, TX.
 Eric Rosenquist
 Elisa Sarino, aka "Elisa" and "ElisaEGO", 27, of San Jose, CA.
 Jeffrey Sasser, aka "Inferno" and "Inferno00", 41, of Charlotte, NC.
 Peter M. Semadeni, aka "Davinci" and "Rev. Wolf", 28, of Overland Park, KS.
 Dean Wuestenberg, aka "Xochi", 44, of Donahue, IA.
 Joseph Yano, aka "Jozef", 34, of Saskatoon, SA.
 Charles Yurek
 Press Release, U.S. Department of Justice, Federal Indictments Returned in Las Vegas Against Software Pirates Nabbed in Operation Bandwidth (June 11, 2002), available at <http://www.cybercrime.gov/bandwidth.htm>;
 Semiannual Report to Congress, October 1, 2002-March 31, 2003, Office of Inspector General of the Environmental Protection Agency 23-24 (May 2003), available at http://www.epa.gov/oigearth/reports/2003/semiannual_20030331.pdf; Semiannual Report to Congress, April 1, 2003-September 30, 2003, Office of Inspector General of the Environmental Protection Agency 21-22 (Nov. 2003), available at <http://www.epa.gov/oigearth/reports/2003/semiannual20031028.pdf>.

¹⁴¹ Press Release, U.S. Department of Justice, Twelve "Operation Bandwidth" Software Pirates Enter into Group Guilty Plea (Dec. 18, 2003), available at <http://www.cybercrime.gov/bandwidthPlea.htm>.

¹⁴² Press Release, U.S. Department of Justice, Federal Indictments Returned in Las Vegas Against Software Pirates Nabbed in Operation Bandwidth (June 11, 2002), available at <http://www.cybercrime.gov/bandwidth.htm>.

¹⁴³ *Id.*

As of January 1, 2004, Operation Digital Piratez has resulted in five publicized convictions.¹⁴⁴ The convictions relate to the following warez servers:

- Wonderland, containing over 5,000 warez with a retail value in excess of \$500,000, operated by Christopher Motter.¹⁴⁵
- City Morgue, containing 1,000 warez totaling 400 gigabytes, operated by Daniel McVay and John Neas.¹⁴⁶
- Only the Finest Warez, which had 100 users and contained 400 gigabytes of warez, operated by Jordan Zielin.¹⁴⁷
- Shayol Ghul, which had 275 users and 17 managers, operated by Kenneth Woods.¹⁴⁸

The prosecutions related to Operation Digital Piratez is ongoing.

g. William Fitzgerald

William Fitzgerald, a 53-year old computer technician for Arlington County, Virginia, obtained warez from IRC and posted them on three computers he ran from his home.¹⁴⁹

Fitzgerald stipulated that the warez were worth between \$40,000 and \$70,000.¹⁵⁰ He pleaded guilty to one count of criminal copyright infringement and received four months in prison and

¹⁴⁴ In a related prosecution, Jonathan Crane, a Qwest employee in Virginia, pleaded guilty to obstructing justice for dismantling servers after learning that a subpoena had been served on Qwest. Jeff Smith, 6 Caught in Piracy Net, Rocky Mountain News (Jan. 27, 2004), *available at* http://www.rockymountainnews.com/drmn/business/article/0,1299,DRMN_4_2606847,00.html.

¹⁴⁵ Press Release, U.S. Department of Justice, Iowa Man Receives Two-Year Prison Sentence in Internet Software Piracy Conspiracy (Sept. 30, 2003), *available at* <http://www.cybercrime.gov/motterSent.htm>.

¹⁴⁶ Press Release, U.S. Department of Justice, Massachusetts Man Pleads Guilty in New Hampshire Software Piracy Conspiracy (Dec. 19, 2003), *available at* <http://www.cybercrime.gov/mcVayPlea.htm>; Press Release, U.S. Department of Justice, Three More Men Plead Guilty in New Hampshire Web-Based Software Piracy Conspiracy (Jan. 23, 2004), *available at* <http://www.cybercrime.gov/zielinPlea.htm> [hereinafter Three More Guilty]; David Tirrell-Wysocki, *Six Plead Guilty to Stealing and Distributing Computer Software*, USA TODAY, Jan. 28, 2004, *available at* http://www.usatoday.com/tech/news/computersecurity/2004-01-26-pirate-days_x.htm.

¹⁴⁷ Three More Guilty, *supra* note 146; Tirrell-Wysocki, *supra* note 146. Jordan Zielin, 30, of Brooklyn, NY, was a Bank of America IT support employee.

¹⁴⁸ Three More Guilty, *supra* note 146; Tirrell-Wysocki, *supra* note 146. Kenneth Woods, 31, of Warrenton, VA, was a Verio Data Center employee.

¹⁴⁹ Statement of Facts, United States v. Fitzgerald, Case No. 0-2620-A (E.D. Va. 2003), *available at* <http://www.usdoj.gov/usao/vae/ArchivePress/FebruaryPDFArchive/fitzgeraldsof020303.pdf>.

¹⁵⁰ Press Release, U.S. Department of Justice, Arlington, Virginia Man Pleads Guilty to Distributing Pirated Software Over the Internet (Feb. 3, 2003), *available at* <http://www.cybercrime.gov/fitzgeraldPlea.htm>.

four months of home confinement.¹⁵¹ Given the Department of Justice's recent large initiatives to take down major warez groups, Fitzgerald's prosecution for relatively small-scale activity is a little puzzling.

h. Operation Safehaven

Operation Safehaven¹⁵² was a 15 month investigation into software piracy. In April 2003, government agents executed over twenty search warrants, leading to the seizure of thousands of CDs and DVDs and various warez servers, including the largest warez site seized in the US to date.¹⁵³ Five defendants have pleaded guilty to conspiracy to commit copyright infringement; three of whom have been sentenced to probation.¹⁵⁴

i. Operation Cybernet

Operation Cybernet targeted the individuals operating the Usenet group alt.2600.arez and other FTP sites and IRC channels.¹⁵⁵ The operation produced its first conviction in December 2003 with the guilty plea of James Remy, a 40 year old from Washington Township,

¹⁵¹ Press Release, U.S. Department of Justice, Arlington County Man is Sentenced to Federal Prison for Distributing Pirated Computer Software over the Internet (Apr. 25, 2003), *available at* <http://www.cybercrime.gov/fitzgeraldSent.htm>.

¹⁵² Press Release, U.S. Department of Justice, Federal Investigation Leads to Prosecution of Internet Software Pirate (Oct. 2, 2003), *available at* <http://www.cybercrime.gov/myersPlea.htm>; *see also* Press Release, U.S. Department of Justice, Operation Safehaven: Hawaii Man Pleads Guilty to Copyright Infringement (Jan. 23, 2004), *available at* <http://www.cybercrime.gov/ishidaPlea.htm>. The individual defendants are; Ross Ishida, 23, aka "daphantm" or "daph," of Honolulu, HI
Terry Katz, 26, of Yorktown Heights, NY
Walter Kapechuk, 55, of Schenectady, NY
Travis Myers, 29, of Yakima, WA
Warren Willsey, 53, of East Berne, NY

¹⁵³ Press Release, U.S. Department of Justice, Federal Investigation Leads to Prosecution of Internet Software Pirate (Oct. 2, 2003), *available at* <http://www.cybercrime.gov/myersPlea.htm>.

¹⁵⁴ *Id.*; *see also* Press Release, U.S. Department of Justice, Operation Safehaven: Hawaii Man Pleads Guilty to Copyright Infringement (Jan. 23, 2004), *available at* <http://www.cybercrime.gov/ishidaPlea.htm>. Sentences are described at *United States v. Kapechuk*, No. 3:03-CR-00279 (D. Conn. 2004); *United States v. Katz*, No. 3:03-CR-00280 (D. Conn. 2004); *United States v. Willsey*, No. 3:03-CR-00281 (D. Conn. 2004).

¹⁵⁵ *See* Press Release, U.S. Department of Justice, Man Admits to Distribution of Pirated Movies, Music, Computer Software and Games Worth Over \$2.2 Million (Dec. 8, 2003), *available at* <http://www.cybercrime.gov/remyPlea.htm>.

NJ.¹⁵⁶ Remy admitted to operating a warez server in his home that, from October 26, 2000 through July 24, 2001, was used to download files with a total retail value of \$2,242,712.¹⁵⁷ The Department of Justice touted this as “the largest loss nationwide in a criminal copyright infringement case resulting from the conviction of a warez site operator who is not part of an organized group.”¹⁵⁸

j. Movie Traders

While not typical warez traders, two individuals have been convicted of distributing pre-release versions of movies. Jason Spatafore distributed parts of *Star Wars Episode I: The Phantom Menace*,¹⁵⁹ for which he sentenced to two years probation.¹⁶⁰ Kerry Gonzalez posted an unfinished “work print” copy of *The Hulk* to a movie bootleg website two weeks prior to the movie’s opening,¹⁶¹ for which he was sentenced to six months home confinement.¹⁶² A third man, Russell Sprague, is being prosecuted for distributing “screener” copies of movies.¹⁶³

7. CASUALTIES IN THE WAR AGAINST WAREZ.

In Congress’ legislative debates about the NET Act, warez traders were portrayed as the poster children for rampant Internet piracy.¹⁶⁴ However, other infringement activities, such as

¹⁵⁶ *See id.*

¹⁵⁷ *Id.*

¹⁵⁸ *Id.* (quoting Assistant U.S. Attorney Christopher J. Christie).

¹⁵⁹ Press Release, U.S. Department of Justice, Man Pleads Guilty to Internet Piracy of Star Wars Film (Dec. 15, 2000), available at <http://www.cybercrime.gov/spataforeplea.htm>.

¹⁶⁰ Jason Spatafore, DisMan’s Online Journey, at <http://www.spatafore.net/disman/thephoenixmenace.shtml> (last visited May 19, 2003).

¹⁶¹ Troy Graham, *Federal Case Made of ‘Hulk’ Piracy*, PHILADELPHIA INQUIRER, June 26, 2003, at H12, available at http://www.philly.com/mld/inquirer/news/local/states/new_jersey/6172522.htm?template=contentModules/printstory.jsp.

¹⁶² Jon Healey, *Man is Sentenced for Posting ‘Hulk’ Film*, L.A. TIMES, Sept. 27, 2003, available at <http://www.latimes.com/technology/la-fi-rup27.5sep27.1.2686007.print.story>.

¹⁶³ Press Release, U.S. Department of Justice, Chicago Man Arrested for Criminal Copyright Infringement in Connection with Prohibited Release of Major Motion Pictures, Many Prior to Their Theatrical Release (Jan. 22, 2004), available at <http://www.cybercrime.gov/spragueArrest.htm>.

¹⁶⁴ *See* 143 CONG. REC. S12689, S12689-91 (daily ed. Nov. 13, 1997) (Senate floor debates); 143 CONG. REC. H9883, H9883-86 (daily ed. Nov. 4, 1997) (House floor debates).

“softlifting” (exceeding a license to make unauthorized copies) and commercial piracy, have a significantly greater impact on copyright owner revenues. So why did Congress target warez traders despite their relatively small footprint on overall piracy?

Despite the obvious inspiration—the *LaMacchia* judge invited Congress to fix the problem¹⁶⁵—another reason may offer a better explanation. Americans hate enemies that are impossible to locate and destroy using command-and-control tactics, and that describes warez traders. Warez traders operate stealthily, behind the Internet’s opaque veil, and are impossible to spot offline. Further, online, warez traders exude an air of cockiness and invincibility that members of Congress may interpret as a provocative challenge to their power and authority.

These attributes make warez traders the unseen enemy that must be destroyed. In a sense, Congress declared war against warez traders through the NET Act. Now Congress wants to triumphantly claim victory over villains who do not fight fair.

While the enemy has suffered a few casualties in Congress’ war against warez, there has been no victory, and it will never come. No quantum of stiffened criminal penalties will change that result. Warez trading is about ego, prestige and reputation, and so long as intangible assets are fenced off, a group of enthusiasts will seek recognition for breaching the fences. In that sense, increased criminal penalties may counterproductively encourage warez trading by making it a little more daring and impressive.

Meanwhile, every war has a collateral cost, and the war against warez is no exception. In the process of outlawing warez trading, Congress also criminalized most American citizens. For

¹⁶⁵ The judge wrote:

Criminal as well as civil penalties should probably attach to willful, multiple indictments of copyright infringement even absent a commercial motive on the part of the infringer. One can envision ways that the copyright law could be modified to permit such prosecution. But, [i]t is the legislature, not the Court, which is to define a crime, and ordain its punishment.

United States v. LaMacchia, 871 F. Supp. 535, 545 (D. Mass. 1994) (quotation omitted), *available at* http://www.loundy.com/CASES/US_v_LaMacchia.html.

example, tens of millions of Americans engage in P2P file sharing,¹⁶⁶ an activity legally indistinguishable from warez trading. But even Americans who do not trade files may break the law simply by willfully infringing \$1,000 of retail value in 180 days, or \$5.56 of willfully infringed copies per day. In our digital society, the average American makes copies, lots of them, every day just to function.¹⁶⁷ The ubiquity of copying makes the dollar standard a criminal threshold that far too many Americans meet easily.

But so what? Systematic noncompliance with the law is a fact of life in our overregulated society, and we have found ways to tolerate or ignore the associated risks. Meanwhile, with stretched prosecutorial resources and the likely futility of prosecuting sympathetic defendants,¹⁶⁸ the risk of an average American being prosecuted for routine acts of copyright infringement is effectively zero. Warez traders get a little more prosecutorial attention,¹⁶⁹ but even the number of small-scale warez traders who have been prosecuted is trivial.

On the other hand, criminal copyright infringement has gone too far, and everyone—even Congress—knows it.¹⁷⁰ By over-criminalizing activities that are required to function in our digital society, criminal copyright law has become unjust, making it impossible for the average American to respect and comply with the law.¹⁷¹

¹⁶⁶ See Mary Madden & Amanda Lenhart, Pew Internet Project Data Memo (July 2003), at 3, *at* http://www.pewinternet.org/reports/pdfs/PIP_Copyright_Memo.pdf (estimating at least 35 million file-sharing downloaders in 2003). Other reputable estimates of file-sharing downloaders have pegged the number at over 60 million. See Press Release, Ipsos-Reid, Americans Continue to Embrace Potential of Digital Music (Dec. 5, 2002), available at <http://www.ipsos-reid.com/pdf/media/mr120402-1.pdf>.

¹⁶⁷ See John Leland, *Beyond File-Sharing, a Nation of Copiers*, N.Y. TIMES, Sept. 14, 2003.

¹⁶⁸ See DOJ IP Crimes Manual, *supra* note 15, § III(E)(4) (advising prosecutors not to proceed with criminal infringement cases against sympathetic defendants unless the prosecutor can show egregious conduct).

¹⁶⁹ See *id.* (discussing the factors that evidence “egregious” Internet infringement).

¹⁷⁰ See Lisa Friedman, Web Pirates Plunder On, L.A. Daily News, June 22, 2003, *at* <http://www.dailynews.com/cda/article/print/0,1674,200%257E20954%257E1471539.00.html> (quoting several members of Congress admitting that legislative efforts to stop piracy have failed).

¹⁷¹ Tom R. Tyler, *Compliance with Intellectual Property Laws: A Psychological Perspective*, 29 N.Y.U. J. INT’L L. 219 (Fall 1996-Winter 1997).

Despite this, the trend is for tougher and more pervasive criminal laws. Over the course of many years, Congress has been convinced by well-funded special interests that the piracy situation is cataclysmic. Thus, Congress regularly holds hearings demanding more pirate busts,¹⁷² and three new bills were introduced into Congress in summer 2003 to toughen up criminal copyright law.¹⁷³ And when Sen. Hatch “jokes” about blowing up the computers of copyright infringers,¹⁷⁴ he is not joking at all—he is expressing frustration at Congress’ seeming inability to get Americans to respect the laws that industry lobbyists have persuaded him and his peers are so desperately needed.¹⁷⁵

To satisfy Congress, the Department of Justice must continue to deliver high-profile criminal copyright convictions. However, to avoid mass panic and undercutting popular support for their mission, the Department of Justice must pursue only cases that permit average

¹⁷² For example, in Spring 2003 the House Judiciary Committee’s Subcommittee on Courts, the Internet and Intellectual Property had three successive hearings in three weeks. *Oversight Hearing on Peer-to-Peer Piracy on University Campuses* (Feb. 26, 2003), available at http://commdocs.house.gov/committees/judiciary/hju85286.000/hju85286_of.htm, *Oversight Hearing on Copyright Piracy Prevention and the Broadcast Flag* (Mar. 6, 2003), available at http://commdocs.house.gov/committees/judiciary/hju85490.000/hju85490_of.htm, and *Oversight Hearing on International Copyright Piracy: Links to Organized Crime and Terrorism* (Mar. 13, 2003), available at http://commdocs.house.gov/committees/judiciary/hju85643.000/hju85643_of.htm.

¹⁷³ See Piracy Deterrence and Education Act of 2003, H.R. 2517, 108th Cong. (2003), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2517ih.txt.pdf (proposing to ramp up enforcement of criminal copyright law); Author, Consumer, and Computer Owner Protection and Security Act (ACCOPS), H.R. 2752, 108th Cong. (2003), available at <http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.2752> (among other provisions, proposing to make the placement of a single copyrighted work in a P2P file-sharing software’s share directory automatically eligible for felony prosecution); Artists’ Rights and Theft Prevention Act of 2003, S. 1932, 108th Cong., § 4 (2003), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s1932is.txt.pdf (among other provisions, proposing to make the placement of a single copy of a pre-release copyrighted work (such as a pre-release version of a movie) in a P2P file-sharing software’s share directory a felony).

¹⁷⁴ Declan McCullagh, Senator OK with Zapping Pirates’ PCs, CNET News.com (June 18, 2003), at http://news.com.com/2102-1028_3-1018845.html?tag=ni_print. Rep. Berman has been quoted as saying “with a smile” that he probably didn’t support the death penalty for piracy. Patrick Ross, DOJ, Hill Subcommittee Agree on Need for Piracy Prosecutions, Warren’s Washington Internet Daily, Mar. 14, 2003, available at 2003 WL 16116847.

¹⁷⁵ Stuntz attributes the underperformance of criminal laws to the mixed signals legislators send when enacting inconsistent and overlapping laws, which undercuts the communicative force of legislative efforts. Stuntz, *supra* note 79, at 520.

Americans to distinguish the criminal's conduct from their own.¹⁷⁶ Unsympathetic warez traders provide a perfect target for the Department of Justice to balance these conflicting objectives.¹⁷⁷ As a result, it seems likely that more warez traders will suffer the consequences of Congress' stubborn desire to change America's addiction to copying.

¹⁷⁶ See generally I. Trotter Hardy, *Criminal Copyright Infringement*, 11 WM. & MARY BILL RTS. J. 305 (2002) (discussing differences in American attitudes towards different types of groups of infringers); Geraldine S. Moohr, *The Crime of Copyright Infringement: an Inquiry Based on Morality, Harm and Criminal Theory*, 83 B.U. L. REV. 731 (2003) (discussing the distinctions between commercial piracy and non-commercial personal infringement).

¹⁷⁷ See Ross, *supra* note 174 (discussing how the Department of Justice has linked warez trading to organized crime and international terrorism).

Appendix A

Publicized Convictions Under the No Electronic Theft Act
(principally updated as of February 11, 2004)¹⁷⁸

Individual	Sentencing Date	Summary of Criminal Activity	Sentence
Jeffrey Levy	August 1999	Posted software, music, entertainment programs and movies with a retail value of at least \$5,000 to his website	2 years probation Internet use restricted
Eric Thornton	December 1999	Posted software with a retail value of at least \$9,638 to his website	5 years probation \$9,638 restitution Must post notice on website for 18 months Cannot use computers (except for business or educational purposes) for 12 months, and Internet use restricted
Brian Baltutat	October 2000	Posted infringing software to a website that was visited by 65,000 people	3 years probation 180 days home confinement (including a tether) \$7,087 restitution 40 hours community service. Cannot use the Internet Required to tell the owners of any computers he uses about his conviction
Jason Spatafore	December 2000	Electronically distributed portions of <i>Star Wars I</i>	2 years probation \$250 fine
Tyrone Augustine (PWA)	April 2002	Intel employee who participated in warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Brian Boyansky (PWA)	April 2002	Intel employee who participated in warez group trading software with retail value of \$1,424,640	5 years probation \$2,000 fine
Diane Dionne (PWA)	April 2002	Senior member of and packager for warez group trading software with retail value of \$1,424,640	5 years probation
John Geissberger (PWA)	April 2002	Intel employee who participated warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Christian Morley (PWA)	April 2002	Packager for warez group trading software with retail value of \$1,424,640	24 months in prison 2 years supervised release [went to trial in May 2001]
Jason Phillips (PWA)	April 2002	Member of warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Brian Riley	April 2002	Intel employee who	5 years probation

¹⁷⁸ This chart is synthesized from sources cited in the main text. Though every attempt has been to make this current as of February 11, 2004, rapidly changing events, spotty media coverage and inconsistent posting of information to databases like PACER undercut accuracy efforts.

(PWA)		participated in warez group trading software with retail value of \$1,424,640	
Jason Slater (PWA)	April 2002	Cracker for warez group trading software with retail value of \$1,424,640.	8 months in prison 6 months community custody 2 years supervised release \$1,000 fine
Mark Stone (PWA)	April 2002	Member of warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Gene Tacy (PWA)	April 2002	Intel employee who participated in warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Todd Veillette (PWA)	April 2002	Member of and senior courier for warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Barry Erickson (Buccaneer)	May 2002	Provided pre-release Symantec software to warez groups RisciISO and DrinkOrDie, founding member of warez group POPZ	33 months in prison (reduced in November 2002 to 15 months) 2 years supervised release
David Grimes (Buccaneer)	May 2002	Provided pre-release Check Point software to DrinkOrDie; operated FTP site High Octane, which was affiliated with warez groups RiSC, MYTH, RTS and DrinkOrDie	37 months in prison (immediately reduced to 16 months in prison) 3 years supervised release Substance abuse treatment
Thomas Oliver (PWA)	May 2002	Council member of warez group trading software with retail value of \$1,424,640	3 years probation \$5,000 fine
Robin Rothberg (PWA)	May 2002	Led and council member of warez group trading software with retail value of \$1,424,640	18 months in prison 3 years supervised release \$1,000 fine
John Sankus (Buccaneer)	May 2002	Led and managed warez group DrinkOrDie, participated in warez group Harm; traded software with retail value of between \$2.5 million and \$5 million	46 months in prison (reduced November 2002 to 18 months) 2 years supervised release 200 hours community service
Nathan Hunt (Buccaneer)	June 2002	Senior member of warez group DrinkOrDie, in 11 month period, provided 120 software programs for cracking and distribution. Stipulated to trading software with retail value of between \$2.5 million and \$5 million	33 months in prison (reduced November 2002 to 24 months) 3 years supervised release \$2,500 fine
Stacey Nawara (Buccaneer)	June 2002	Senior member of warez group RTS, Council	30 months in prison (reduced in October 2002 to 30 days in jail (straight time or weekends))

		member of warez group DrinkOrDie, courier for warez group Razor1911	and 8 months community confinement)) 3 years supervised release Assigned to mental health and substance abuse program \$1,000 fine No non-work Internet use
Richard Berry (Buccaneer)	July 2002	Longtime member of DrinkOrDie, provided them hardware, tested cracked warez and operated bounce sites	33 months in prison (reduced in October 2002 to 2 years probation including 12 months home confinement with electronic monitoring) 2 years supervised release
Andrew Clardy (Buccaneer)	July 2002	System administrator for DrinkOrDie's Dynamo server	41 months in prison 2 years supervised release
Michael Kelly (Buccaneer)	July 2002	Senior staff of DrinkOrDie, member of warez groups RISC, AMNESIA, CORE	33 months in prison 2 years supervised release 200 hours community service Must notify employers of conviction In January 2003, the sentence was reduced to: 4 months in prison 3 years supervised release (including 8 months home detention with electronic monitoring) 200 hours community service Must notify employers of conviction
Sabuj Pattanayek (Buccaneer)	July 2002	Council member of and cracker for warez group DrinkOrDie, senior member of warez group RTS	41 months in prison 3 years supervised release 100 hours community service \$1,000 fine In May 2003, his sentence was reduced to: 3 years probation 6 months community confinement 200 hours community service Fine
John Riffe (Buccaneer)	July 2002	Member of warez groups ShadowRealm (SRM), EXODUS	2 years probation 6 months home confinement with electronic monitoring 100 hours community service
Tony Walker (Fastlane)	July 2002	Provided computer hardware to warez group Fastlane in exchange for access to software with retail value of \$1,000,000	5 months in prison (split with community confinement) 1 year supervised release \$3,000 fine [went to trial March 2002]
Anthony Buchanan (Buccaneer)	August 2002	Participated in warez groups POPZ and DrinkOrDie	2 years probation 6 months home confinement with electronic monitoring 150 hours community service
Steve Deal (Fastlane)	August 2002	Led warez group trading software with retail value of \$1,000,000	30 months in prison 3 years supervised release
Robert Gross (Buccaneer)	August 2002	Participated in warez group DrinkOrDie	5 years probation 6 months home confinement 200 hours community service
Glendon Martin	August 2002	System administrator for	3 years probation

(Fastlane)		warez group trading software with retail value of \$1,000,000	\$1,000 fine
Shane McIntyre (Fastlane)	August 2002	Managed warez group trading software with retail value of \$1,000,000	3 years probation 180 days home confinement with electronic monitoring \$3,000 fine
James Milne (Fastlane)	August 2002	System administrator for warez group trading software with retail value of \$1,000,000	3 years probation
Bjorn Schneider (Fastlane)	August 2002	Managed warez group trading software with retail value of \$1,000,000	3 years probation
Christopher Tresco (Buccaneer)	August 2002	System administrator for DrinkOrDie (including operating a drop site)	33 months in prison (reduced in October 2002 to 6 months in prison and 7 months community confinement) 2 years supervised release 100 hours community service May not use the Internet for non-work related purposes
Kevin Vaughan (Fastlane)	August 2002	System administrator for warez group trading software with retail value of \$1,000,000	3 years probation
Tae Yuan Wang (Fastlane)	August 2002	Managed warez group trading software with retail value of \$1,000,000	3 years probation 300 hours community service
Steven Ahnen (PWA)	September 2002	Council member for warez group trading software with retail value of \$1,424,640. Alleged to operate channel for the group and package software	3 years probation \$1,000 fine
Derek Eiser (Buccaneer)	September 2002	Participated in warez group DrinkOrDie	2 years probation, including 6 months home confinement \$500 fine
David Anderson (Buccaneer)	October 2002	Participated in warez group DrinkOrDie	12 months probation \$500 fine
Myron Cole (Buccaneer)	October 2002	Participated in warez group DrinkOrDie	2 years probation 150 hours community service
Justin Robbins (PWA)	October 2002	Council member of warez group trading software with retail value of \$1,424,640; supplied Microsoft software and allowed others to access Microsoft's internal network	7 months in prison 3 years supervised release
Ruth Lawton (Bandwidth)	December 2002	Downloaded more than \$2,500 of infringing works to her home computer	3 years probation \$2,000 fine
Ryan Breeding (Fastlane)	February 2003	Provided computer hardware to warez group Fastlane in exchange for access to software with retail value of \$1,000,000	15 months in prison 2 years supervised release \$6,000 fine

Eric Rosenquist (Bandwidth)	March 2003	Downloaded Microsoft Money to his home computer	3 years probation 140 hours community service \$500 fine
Lukasz Doupal (Bandwidth)	April 2003	Participated in warez group Rogue Warriorz (RWZ)	3 years probation \$2,000 fine
William Fitzgerald	April 2003	Operated website allowing downloads of between \$40,000 and \$70,000	4 months in prison 4 months home confinement \$3,000 fine
Shane Pitman (Buccaneer)	June 2003	Leader of warez group Razor1911	18 months in prison (reduced in August 2003 to 12 months plus one day) 3 years supervised release
David Russo (Buccaneer)	July 2003	Tester for warez group DrinkOrDie	To be determined
Brad McGourty (Bandwidth)	August 2003	Participant in Rogue Warriorz (RWZ); admitted to downloading Microsoft Money to home computer	1 year probation \$500 fine \$60 restitution
Charles Yurek (Bandwidth)	August 2003	Participant in Rogue Warriorz (RWZ); admitted to downloading Windows XP to home computer	6 months of electronically monitored home detention 3 years probation \$500 fine
Kent Kartadinata (Buccaneer)	September 2003	Operated email server for warez group DrinkOrDie	5 years probation 2,400 hours community service in anti-piracy program
Mike Nguyen (Buccaneer)	September 2003	Managed file servers for warez group DrinkOrDie	5 years probation 2,400 hours community service in anti-piracy program
Kerry Gonzalez	September 2003	Distributed advance "work print" copy of <i>The Hulk</i>	6 months home confinement 3 years probation \$2,000 fine \$5,000 restitution
Christopher Motter (Digital Piratez)	September 2003	Operated warez server Wonderland with 5,000 warez worth at least \$500,000	24 months in prison
John Amorosi (Bandwidth)	January 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Walter Kapechuk (Safehaven)	February 2004	Operated warez servers at SUNY Albany	3 years probation 200 hours community service \$6,000 fine
Terry Katz (Safehaven)	February 2004	System operator for warez servers	4 years probation (first 3 months in halfway house) \$6,000 fine
Mark Shumaker (Buccaneer)	February 2004	Led music piracy site Apocalypse Crew and supplied content to warez group DrinkOrDie; stipulated infringement of between \$40,000 and \$70,000	To be determined
Warren Willsey (Safehaven)	February 2004	Periodically helped maintain warez servers at SUNY	1 year probation \$1,000 fine

		Albany	
Wolf Bachenor (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
David Brandt (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Alexander Castaneda (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Jacob Clappton (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Jonathan Dow (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Jorge Garcia (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Mark Konarske (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Timothy Lastoria (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
David Lowe (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Christopher Mastrangelo (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Daniel McKay (Digital Piratez)	March 2004	Operated warez server City Morgue with 1,000 warez items	To be determined
Suzanne Peace	March 2004	Participated in warez group	To be determined

(Bandwidth)		Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	
James Remy (Cybernet)	March 2004	Operated warez server that had \$2,242,712 of infringing downloads	To be determined
Lindle Romero (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Elisa Sarino (Bandwidth)	March 2004	Participated in warez group Rogue Warriorz (RWZ), which infringed works with a retail value over \$1,000,000	To be determined
Ross Ishida (Safehaven)	April 2004	Operated a warez server through the University of Hawaii and was a courier for warez groups	To be determined
John Neas (Digital Piratez)	April 2004	Operated the warez server City Morgue with 81 users and 400 GB of warez	To be determined
Kenneth Woods (Digital Piratez)	April 2004	Operated the warez server Shayol Ghul, with 275 users and 17 managers, through Verio's network	To be determined
Jordan Zielin (Digital Piratez)	April 2004	Operated the warez server Only the Finest Warez, with 100 users and 400 GB of warez, through a Bank of America network	To be determined
Travis Myers (Safehaven)	August 2004	Courier for several warez groups, including DrinkOrDie	To be determined